

## CLAIMS

1           1.       A method for providing secure authentication of a user to a system and  
2       secure operation of the system thereafter, the method comprising:  
3           authenticating a user to the system directly or via a proximity device;  
4           authenticating the proximity device to a receiver in the system;  
5           upon successful authentication, initiating operation of the system; and  
6           intermittently communicating between the proximity device and the receiver to  
7       verify whether the proximity device is within continued proximity of the system.

1           2.       The method of claim 1, further comprising:  
2           if the user is not authenticated to the proximity device after a predetermined  
3       number of attempts, garbling sensitive information stored in the proximity device.

1           3.       The method of claim 1, further comprising:  
2           communicating a distress signal, if it is determined that the proximity device is  
3       not operating in proximity of the system.

1           4.       The method of claim 1, further comprising:  
2           beginning operation of the system in a fail-safe mode if it is determined that  
3       the proximity device is not operating in proximity of the system.

1           5.       The method of claim 1, wherein the proximity device is one of the  
2 following: a personal digital assistant (PDA), a cellular phone, a pager, a smart card, a  
3 pocket PC, an audio-video device, a laptop, a tablet PC, a camera, or a portable device  
4 carried by a courier.

1           6.       The method of claim 1, wherein authenticating the user to the system  
2 or to the proximity device comprises at least one or a combination of the following:  
3 receiving user identification (ID) information, scanning the user's finger print,  
4 recognizing the user's facial characteristics, recognizing the user's voice, verifying a  
5 user's DNA, and verifying biometrics of the user.

1           7.       The method of claim 1, wherein authenticating the proximity device to  
2 the receiver comprises at least one or a combination of the following: a challenge-  
3 response algorithm, a digital signature algorithm, a public-private key algorithm, a  
4 one-time password algorithm, and a symmetric key algorithm.

1           8.       The method of claim 1, wherein authenticating the proximity device to  
2 the receiver comprises one of: communicating via a wireless interface or via a wired  
3 interface.

1           9.       A system for user authentication to a machine and secure operation of  
2 the machine thereafter, the system comprising:  
3           a receiver coupled to, or integrated with, the machine; and  
4           a proximity device, comprising;  
5                   means for authenticating a user to the proximity device;  
6                   means for authenticating the proximity device to the receiver; and  
7                   means for, upon successful authentication, intermittently  
8 communicating between the proximity device and the receiver to verify whether the  
9 proximity device is within proximity of the machine.

1           10.     The system of claim 9, wherein the receiver comprises:  
2           means for determining whether the proximity device is in proximity of the  
3 machine; and  
4           means for beginning operation of the machine in a fail-safe mode if it is  
5 determined the proximity device is no longer operating within proximity.

1           11.     The system of claim 10, wherein the receiver further comprises:  
2           means for initiating communication of a distress signal to a receiving station  
3 upon beginning operation in a fail-safe mode.

1           12.     The system of claim 9, wherein the proximity device is one of the  
2 following: a personal digital assistant (PDA), a cellular phone, a pager, a smart card, a  
3 pocket PC, an audio-video device, a laptop, a tablet PC, a camera, or a portable device  
4 carried by a courier.

1           13.     The system of claim 9, wherein the means for authenticating a user to  
2     the proximity device comprises at least one of the following: means for receiving user  
3     identification (ID) information, means for scanning the user's finger print, means for  
4     recognizing the user's facial characteristics, means for recognizing the user's voice,  
5     means for verifying a user's DNA, means for recognizing body temperature, means  
6     for recognizing blood pressure, and means for verifying biometrics of the user.

1           14.     The system of claim 9, wherein the means for authenticating the  
2     proximity device to the receiver comprises at least one of the following: means for  
3     processing a challenge-response algorithm, means for processing a digital signature  
4     algorithm, means for processing a public-private key algorithm, means for processing  
5     a one-time password algorithm, means for processing the identity of the user, and  
6     means for processing a symmetric key algorithm.

1           15.     The system of claim 9, wherein the proximity device further comprises:  
2     means for storing identification information about at least a first user.

1           16.     A device for providing authentication of a user to a system and for  
2     providing secure operation of the system thereafter, the device comprising:  
3     memory for storing identification information of at least a first user;  
4     an interface for authenticating a user;  
5     an interface for authenticating the device to a receiver integrated with the  
6     system; and  
7     logic configured to intermittently communicate with the receiver upon  
8     successful authentication.

1           17.     The device of claim 16, wherein the interface for authenticating the  
2     device to the receiver is a wireless interface.

1           18.     The device of claim 16, wherein the interface for authenticating the  
2     device to the receiver is a wired interface.

1           19.     The device of claim 16, further comprising:  
2             logic configured to garble secure information upon a predetermined number of  
3     failed attempts at authenticating the user.

1           20.     The device of claim 16, further comprising:  
2             logic configured to operate the device in a sleep mode, such that minimal  
3     power needed to maintain intermittent communications with the receiver is utilized.